UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of Information Associated with Kik Account DrOral420, that is stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab.ai, Inc., located at 1237 7th Street, Santa Monica, California 90401.	Case No. 4:22 MJ 8086 SRW SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 U.S.C. § 2252A(a)(1) and (2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (access with intent to view and possession of child pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

THOMAS H PUTTING
Digitally signed by THOMAS H PUTTING
Date: 2022.03.17 12:50:43 -05'00'

Applicant's signature

Thomas Putting, Special Agent

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 03/18/2022

Judge's signature

City and state: St. Louis, MO

Honorable Stephen R. Welby, U.S. Magistrate Judge

Printed name and title

AUSA: Robert F. Livergood

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF Information Associated with Kik Account **DrOral420**, that is stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab.ai, Inc., located at 1237 7th Street, Santa Monica, California 90401.	No. 4:22 MJ 8086 SRW SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a Special Agent with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with KIK account **"DrOral420"** (the "subject account") that is stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab.ai, Inc., (formerly "KiK Interactive, Inc.") a social-networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require Kik c/o Medialab.ai, Inc. to disclose to the United States records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the subject account as further described in Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations ("HSI"), since March 2019, and am currently assigned to the HSI office in Saint

Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 1470, 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) and (2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (access with intent to view and possession of child pornography) (hereinafter the "SUBJECT OFFENSES") are presently located in **the TARGET ACCOUNT**, further described in Attachment A, for the things described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched is: Kik Account **DrOral420,** that is stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab.ai, Inc., located at 1237 7th Street,

Santa Monica, California 90401, further described in Attachment A. The items to be reviewed and seized by the United States are described in Attachment Part II of Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States (including a magistrate judge of such court). . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i)."

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Geo-located," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

d. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, sharing photos or videos, reading a book, or playing a game.

f. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

g. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

h. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

COMPUTERS AND CHILD PORNOGRAPHY

8. From my own training and experience in the area of Internet-based child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true. Computers connected to the Internet identify each other by an Internet Protocol ("IP") address. An IP address can assist law enforcement in finding a

particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

9. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and wireless telephones, child pornography is traded through the Internet, by using, for example, file sharing software.

10. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, as well as from a wireless telephone. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

11. The Internet allows any computer (including wireless telephone) to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs which allow subscribers to connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their

own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

12. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

BACKGROUND ON KIK

13. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

14. An "Internet Protocol" (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to

the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

15. An "Internet Service Provider" (ISP) is an entity that provides access to the Internet to its subscribers.

16. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

17. Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos, and more-all within the application. Kik is available for download through the iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages.

18. Unlike many other smartphone messaging services which are based on a user's phone number, Kik uses usernames as the unique identifier. By using the usernames instead of phone numbers, users' personal information is never shared by Kik. If a Kik user is an active user of other social apps and sites, they might choose to share their username on those sites to connect with their followers from there. If a user posts his/her Kik username somewhere like Twitter or Instagram, or on a Kik optimized webpage, will make it publicly available.

19. The "New Chats" feature gives users control over who they talk to. This safety feature puts messages from new people in a separate section called "New Chats." In messages from new people, picture, or content messages they may have sent are blurred, with the option to unblur and view the content. A user has the option to either start a chat with them, delete, block, or report.

20. A Kik username is unique, can never be replicated, can never be changed, and is the only publicly available identifier used to identify a Kik account. Kik cannot identifier users using phone numbers, first and last name (display name), or email address. The exact Kik username must be provided to conduct any search in the Kik system.

21. A "Group Hashtag" (Public Groups) is a user-generated hashtag, can never be replicated, can never be changed, and will begin with the hashtag symbol (#).

22. A Group Scan Code can be used for private and public groups. It can be accessed through the group profile information page and users can share the scan code to invite others to join.

23. JIDs are unique internal IDs associated to users and group chats, randomly generated by Kik's internal systems. JIDs are not public-facing. A user JID is a username followed by an underscore and three additional characters that are randomly assigned by Kik for every username. A group JID is a 13-digit numeric string followed by "_g." It will not contain alphabetical characters (other than the "_g"), periods, spaces, or emoticons.

24. A content ID is a unique ID associated to a media file sent on Kik. The format of a Kik content ID is eight alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, twelve alphanumeric characters.

25. As explained herein, information stored in connection with a Kik account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Kik user's account activity, IP log, stored electronic communications, and other data retained by Kik,

can indicate who has used or controlled the Kik account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Kik "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Kik account owner. Last, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

26. Based on the information above, the computers of Kik c/o Medialab.ai, Inc. are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, which would include information such as the IP

addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

PROBABLE CAUSE

27. On or about December 29, 2021, law enforcement in the UK notified Homeland Security Investigations (HSI) Cyber Crimes Center (C3) in the United States of a subject in the United States talking to an individual who identified themselves as a twelve (12) year-old female, hereafter referred to as M.F.1, living in the UK.[1] The subject utilizing KIK and using username DrOral420, who was later identified as **Corey WADEL**, was in contact with M.F.1. between November 11, 2021, and December 16, 2021. WADEL appeared to initiate contact with M.F.1 and stated his age as thirty-four (34) years old. M.F.1 stated their age was twelve (12) years old, to which WADEL stated "Nice". "Bet you look really pretty too". M.F.1 replied back "Dw if Im to young to char to", to which WADEL stated "Not at all. I like young pretty ladies", "Would love to see what you look like <kissing face emoji>. WADEL continued the conversation stating he would like to be M.F.1's daddy and commented "Just mean I would love a young girl like yourself for my own pleasures haha", and stated he would like to touch M.F.1's private areas. WADEL made another comment of "If I had a daughter like you I would take care of her every night. Give you kisses everywhere.". M.F.1 asked WADEL if he had a daughter, to which WADEL stated he has a one (1) year-old and then stated, "I just mean that I can't play with her little vagina the way

[1] M.F.1 is an actually an Undercover Investigator (UC) within the United Kingdom law enforcement. The name used in the conversation with WADEL, and the username used by the UC on the KIK application is known to your affiant but is withheld from this application since the undercover operation is still ongoing and could compromise the investigation. I have reviewed the conversations and included pertinent conversations herein.

I want to play with yours". Later in the conversation WADEL stated he did sexual thing with his cousin who was thirteen (13) years old while WADEL was twenty-one (21) years old.

28. During the chat with M.F.1, WADEL stated he worked for a juvenile detention center. This was verified by Kirksville Police Department on January 7, 2022.

29. WADEL during the chat with the minor female sent unsolicited pictures of his genitals. Description of the images sent by WADEL are described below:

a. "14321d5b-1804-48e7-9e6d-d0f11ad8e97d" - this is a graphic video file, approximately seventeen (17) seconds in length, that depicts, in part, an adult male, who is wearing either a plaid pajama bottoms or a plaid blanket, masturbating. The adult male's penis and hand are the only part of the male visible in the video.

b. "02d80861-a979-4421-8149-c99f92a26efa" - this is a graphic image file, that depicts, in part, an adult nude male in what appears to be a shower, with the male's genitals the focus of the image.

c. "c511b595-4ae5-4a6e-902b-cd59b2e2b444" - this is a graphic image file, that depicts, in part, an adult male wearing a blue shirt with white writing and either plaid pajamas or a plaid blanket. The adult male has his erect penis as the center point of the image.

d. "49e9c7f5-dd79-4bd1-a619-984d24c96daa" - this is a graphic image file, that depicts, in part, an adult male, who is wearing a plaid shirt and blue jeans, holding his penis and testicles in his hand.

30. On or about December 6, 2021, HSI London UK served ICE Administrative Summons (ICE-OIA-LN-2022-00044) to Kik Interactive, Incorporated for subscriber data on KIK

user DrOral420. On or about December 13, 2021, KIK responded with the following subscriber information.

First Name:	Proud
Last Name:	Daddy
Username:	DrOral420
Email:	cwadel2987@gmail.com
Birthday:	/1987
Registration Device:	iPhone

KIK also supplied a list of IP addresses used and their date and times. One of the most common used IP addresses used between November 11, 2021, and December 16, 2021, was 108.95.126.243.

31. On January 3, 2022, your affiant was assigned the Corey WADEL case that stemmed from information received by United Kingdom (UK) law enforcement.

32. On or about January 24, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-00079) to AT&T, Inc., for subscriber information on IP address 108.95.126.243 used between November 11, 2021, to December 16, 2021.

33. On or about January 28, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-00080) to Google, Inc., for subscriber information on email address cwadel2987@gmail.com. On or about January 28, 2022, Google responded to the summons with the following information:

Name:	Corey A WADEL
Given Name:	Corey A
Family Name:	WADEL
Account:	77419097039
e-mail:	cwadel2987@gmail.com
Created on:	11/03/2016
Terms of Service:	98.30.248.109
Last Updated On:	07/19/2021
Recovery SMS:	269-235-4186
Recovery Phone:	269-235-4186

Google, Inc., also supplied Google Pay information:

Payments Profile ID:	9087-1809-3325
Contact Email:	cwadel2987@gmail.com
Admin Emails:	cwadel2987@gmail.com
Address:	703 West Hickory St, Kirksville, MO 63501

34. On January 28, 2022, your affiant queried a public database system. The query revealed that WADEL used to reside at 703 West Hickory St, Kirksville, MO 63501 from approximately March 2018 to May 2019.

35. On or about January 28, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-00083) to AT&T, Inc., for subscriber information on telephone number 269-235-4186. On or about January 30, 2022, AT&T, Inc., responded to the summons with the following information:

Financial Liable Party

Name:	Corey WADEL
Credit Address:	702 W Laharpe St, Kirksville, MO 63501
Activation:	10/16/2015

Billing Party:

Account Number:	917720823
Name:	Corey WADEL
Billing Address:	702 W Laharpe St, Kirksville, MO 63501
Account Status:	Cancelled
MSISDN Active:	10/16/2015 to 10/01/2017

This MSISDN is no longer associated with WADEL. However, it was associated to him when Google account cwadel2987@gmail.com was created on November 3, 2016.

36. On or about January 24, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-00079) to AT&T Inc, for subscriber information on IP address

108.95.126.243 used between November 11, 2021, to December 16, 2021. On or about January 30, 2022, AT&T, Inc., responded to the summons with the following information:

Contact Name:	Corey WADEL
CBR:	419-466-2598
Preferred email:	cwade13187@icloud.com
Account ID:	316220058
Account Name:	Corey WADEL
Established:	09/21/2021
Service Address:	1915 Osteopathy, Kirksville, MO 63501
Billing Address:	1915 Osteopathy, Kirksville, MO 63501

37. Your affiant checked public database systems on or about January 28, 2022, which revealed that an individual named Corey Alexander WADEL with a Date of Birth of XX XX, 1987, resides at 1915 Osteopathy Lot 13, Kirksville, MO 63501.

38. On January 20, 2022, a Kirksville City Police Department (KCPD) Officer conducted surveillance of the 1915 Osteopathy Lot 13, Kirksville, MO 63501 and observed a black Honda Pilot bearing Missouri license plate "EF4S4V". A check with a public database system revealed the vehicle was registered to Corey WADEL and Christopher Weller.

39. On January 28, 2022, representatives of Ameren contacted your affiant and stated the services for the 1915 Osteopathy, Kirksville, MO 63501 is current since June 2019 and that the responsible party is Corey WADEL.

40. On February 14, 2022, your affiant obtained a search warrant for WADEL's residence at 1915 Osteopathy Lot 13, Kirksville, MO 63501. The search warrant authorized your affiant to search and seize any evidence, instrumentalities, and contraband pertaining to the violation of Title 18, United States Code, Section 1470, knowingly transferring obscene material to a minor under 16 years of age or attempting to do so.

41. On February 16, 2022, your affiant executed the search warrant at 1915 Osteopathy Lot 13, Kirksville, MO 63501. Your affiant seized the following items: (1) an Acer Tablet found

in the bedroom; (2) an iPhone with bluish/green back found on WADEL's person; (3) an iPhone A1586 found in the kitchen; (4) Black Alcatel One Touch cellphone found in the bedroom behind some clothes; and (5) Blue Thumb Drive found in a dresser in the bedroom.

42. During the search warrant your affiant had a consensual interview with WADEL. Below is not a verbatim account but a summary of the interview.

a. During the interview WADEL gave his password to his cellphone. WADEL then stated he used an application called "KIK". WADEL stated he assumes the people he talks to are "18 and up" but then stated the only thing that could get him (WADEL) in trouble is pictures. Your affiant asked WADEL what kind of conversations he (WADEL) was having on KIK. WADEL stated he has been added to groups where people have posted Mega Links.[2] WADEL stated he has a Mega account and some of the links he (WADEL) received depict images/videos of people under the age of 18 years. WADEL stated he could be in trouble for those images and that he should have "some of those".

b. WADEL then stated he would like to have a lawyer. The interview was then concluded, and no other questions were asked to WADEL.

43. When the search warrant was concluding and your affiant was conducting the inventory in front of WADEL, WADEL, without any prompting by your affiant, stated there could be images of underage children in his phone and on his accounts. WADEL then stated that people would send him links and that the only way to find out what the link was, was to download the link. WADEL then stated he never got around to deleting the images from those links.

[2] Mega Links are links used by Mega, a cloud-based storage service, users to share files from the user's cloud base storage account. These Mega Links can be used in a non-criminal activity but, as your affiant has witnessed in other investigations, has been used to distribute child pornography.

44. During the search of WADEL's phone, your affiant viewed the KIK application on the phone. Your affiant then viewed on the KIK application the TARGET ACCOUNT, to include a profile picture of a toddler female that matches an image sent to M.F.1 in the conversation above.

45. It is your affiant's belief that WADEL is the owner of the TARGET ACCOUNT based on the information stated above, and within that account the conversation stated above with M.F.1 along with child pornography, per WADEL's utterances, will be found in the TARGET ACCOUNT.

CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND COLLECT IMAGES OF CHILD PORNOGRAPHY

46. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area, or in the "cloud." These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in the "cloud," to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer to have continuous access to their collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

47. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses

of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A), by using the warrant to require Kik c/o Medialab.ai, Inc. to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Kik. Because the warrant will be served on Kik, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

51. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

THOMAS H PUTTING
Digitally signed by THOMAS H PUTTING
Date: 2022 03.17 12:50:14 -05'00'

THOMAS PUTTING
Special Agent
Homeland Security Investigations

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 18th day of March 2022.

STEPHEN R. WELBY
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

Property to Be Searched

This warrant applies to information associated with the Kik profile with username: DrOral420, that is stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab.ai, Inc., located at 1237 7th Street, Santa Monica, California 90401.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

List of Items to be Seized

I. Information to be disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, messages, images, videos, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each **Subject Account** or identifier listed in Attachment A:

Non-Content User Data

(a) Basic Subscriber data;

(b) Current first and last name and email address;

(c) Link to the most current profile picture or background photo;

(d) Device related information;

(e) Account creation date and Kik version;

(f) Birthdate and email address used to register the account;

(g) User location information, including IP address(es).

Content Data

(a) IP addresses associated to the Kik account **DrOral420** from **November 1, 2021, to February 28, 2022**;

(b) All transactional chat logs associated to the Kik account **DrOral420** from **November 1, 2021, to February 28, 2022**;

(c) All images and video associated to the Kik account **DrOral420** including the unknown usernames and IP address associated to the sender of the images and video from **November 1, 2021, to February 28, 2022,**;

(d) A date-stamped log showing the usernames that Kik account **DrOral420** added and/or blocked from **November 1, 2021, to February 28, 2022**;

(e) All abuse reports associated to the Kik account **DrOral420** including the unknown usernames from **November 1, 2021, to February 28, 2022;**

(f) All emails associated to the Kik account **DrOral420** from **November 1, 2021, to February 28, 2022**;

(g) Registration IP address associated to the Kik account **DrOral420**;

(h) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;

(i) All location data associated with the account created, uploaded, or shared by the account;

(j) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(k) All past and current usernames associated with the account;

(l) All records of Kik searches performed by the account, including all past searches saved by the account;

(m) All activity logs for the account and all other documents showing the user's posts and other Kik c/o Medialab.ai, Inc. activities;

(n) All photos and videos uploaded by that account and user ID and all photos and videos uploaded by any user, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(o) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account and user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(p) All IP logs, including all records of the IP addresses that logged into the account;

(q) The types of service utilized by the user;

(r) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(s) All privacy settings and other account settings, including privacy settings for individual posts and activities, and all records showing which Kik users have been blocked by the account;

(t) A list of all of the people that the user follows on Kik and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;

(u) A list of all users that the account has "unfollowed" or blocked;

(v) All privacy and account settings;

(w) All information about connections between the account and third-party websites and applications; and,

(x) All records pertaining to communications between Kik c/o Medialab.ai, Inc. and any person regarding the user or the user's Kik account, including contacts with support services, and all records of actions taken, including suspensions of the account.

(y) Any and all cookies associated with or used by any computer or web browser associated with the account, including the IP addresses, dates, and times associated with the recognition of any such cookie.

Kik c/o Medialab.ai, Inc. is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and (a)(5)(B) (involving transportation, possession of, and accessing with intent to view child pornography), those violations involving KIK user DrOral420, including information pertaining to the following matters:

1. The production of child pornography;

2. The receipt of child pornography;

3. The possession of child pornography;

4. Any information or records reflecting associates, accomplices or conspirators;

5. Any information or records reflecting the sources child pornography and individuals involved in the production, receipt, possession or access with intent to view child pornography;

6. Evidence indicating how and when user's account was accessed to determine the chronological context of account use, account access, and events relating to the crime under investigation;

7. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.